D9 - copy for applicant

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 May 2002 (23.05.2002)

PCT

(10) International Publication Number
WO 02/41101 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US01/43087

(22) International Filing Date:
14 November 2001 (14.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/711,932 15 November 2000 (15.11.2000) US

(71) Applicant: NETCHARGE.COM, INC. [US/US]; Suite 202A, 2201 East Camelback Road, Phoenix, AZ 85016 (US).

(72) Inventor: MOORE, Scott, C.; 614 North St. Paul, Mesa, AZ 85205 (US).

(74) Agents: BOSWELL, Mary, Jane et al.; Morgan, Lewis & Bockius LLP, 1800 M Street, NW, Washington, DC 20036 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/41101 A2

(54) Title: METHOD AND SYSTEM FOR TRANSMITTING DATA WITH ENHANCED SECURITY THAT CONFORMS TO A NETWORK PROTOCOL

(57) Abstract: A method and system for transmitting data with enhanced security that conforms to a network protocol. A first data segment having encrypted data, an unencrypted packet identifier identifying the encrypted data, an unencrypted data identifier associated with an encryption key used to encrypt the encrypted data in the first data segment, and a fourth data segment having data to verify integrity of transmission are encoded to conform to a network protocol. The encoded data segments and encryption key are transmitted. The data segments are received and decoded. The encrypted data is decrypted using the encryption key that corresponds to the data identifier.

METHOD AND SYSTEM FOR TRANSMITTING DATA WITH ENHANCED SECURITY THAT CONFORMS TO A NETWORK PROTOCOL

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a method and system for transmitting data with enhanced security, and more particularly, to method and system for encoding encrypted and unencrypted data to conform to a network protocol.

Discussion of the Prior Art

The Internet continues to grow in popularity as an easy-to-use and effective medium for transmitting information. As the numbers of users of the Internet grows and as the amount of information transmitted continues to grow, the efficient and secure transmission of information has become a concern for many users.

Networks, which are channels for carrying data segments, are configured to operate in accordance with one or more network protocols. The protocol enables different devices attached to the network or in communication with the network to exchange data. Hypertext Transfer Protocol (HTTP) is one of the most commonly used network protocols for transmitting data across the Internet. Other common network protocols include File Transfer Protocol (FTP), Simple Mail Transfer protocol (SMTP), and Secure HTTP (SHTTP). The most popular protocols in the Internet environment transmit data in an URL-encoded format that requires significant bandwidth or transmission capacity. Therefore, it would be advantageous

to provide a method and system for transmitting the same amount of information using fewer bytes of information over existing networks.

Besides the need to transmit data in a more efficient manner, the protection of confidential information on an open network such as the Internet also is needed. This heightened protection concerns users, especially consumers conducting financial transactions on the Internet. To transfer sensitive information across wide area networks, such as the Internet, various security measures have been developed to prevent unsolicited access to the information. One popular security technique is encryption, which involves scrambling data with a unique encryption key. The resulting encrypted data is transmitted to a recipient, who decrypts the data with the unique key.

One potential problem associated with existing encryption techniques is the secure transmission of the encryption key to the recipient. Conventional security protocols, such as Secure Socket Layer (SSL) and SHTTP, fail to provide for a confidential and secure method of distributing keys. The encryption keys are typically transmitted over the Internet, a non-secure network, thereby exposing the keys to unauthorized users who could potentially intercept and decrypt the confidential information.

It would be advantageous to provide a method and system for securely transmitting encrypted data, preferably binary data, using well known protocols such as HTTP, SHTTP, SMTP, and FTP.

SUMMARY OF THE INVENTION

Accordingly, the present invention is directed to a method and system for the efficient and secure transmission of data over a wide area network that substantially obviates one or more of the problems due to limitations and disadvantages of the related art.

One object of the present invention is to provide a method and system for reducing network capacity by transmitting information in unsupported formats using existing network protocols.

Another object of the present invention is to provide a method and system for encrypting and encoding binary data to conform to particular network protocols.

A further object of the present invention is to provide a method and system for transmitting data that is compatible with different hardware architecture.

Yet another object of the present invention is to securely transmit binary data using network protocols that do not support raw binary transmissions.

Another object of the present invention is to provide a method and system for transmitting encrypted and unencrypted data with enhanced security.

Another object of the present invention is to enable the transmission of data formats unsupported by existing protocols that does not require additional network administrative resources.

Additional objects and advantages of the invention will be set forth in the description which follows, and in part will be apparent from the description, or may be learned by practice of the invention. The objectives and other advantages of the invention will be realized and attained by the structure particularly pointed out in the written description and claims hereof as well as the appended drawings.

To achieve these and other advantages and in accordance with the purpose of the present invention, as embodied and broadly described, in one aspect of the present invention there is provided a method for transmitting data with enhanced security that conforms to a network protocol that comprises providing data segments including a first segment having encrypted data, an unencrypted packet identifier identifying the encrypted data, an unencrypted data identifier associated with an encryption key used to encrypt the encrypted data in the first data segment, and a fourth data segment having data to verify integrity of transmission; encoding the data segments to conform to a network protocol; transmitting the data segments and encryption key; receiving and decoding the data segments; and decrypting the encrypted data using the encryption key that corresponds to the data identifier.

In another aspect, the present invention provides a system for transmitting data with enhanced security that conforms to a network protocol that includes means for encrypting data with an encryption key and associating a data identifier with the encryption key; means for associating a packet identifier with the encrypted data; means for encoding the packet identifier, data identifier, and data into a format compatible with a network protocol; means for receiving and decoding the packet identifier, data identifier, and data; and means for retrieving the encryption key that corresponds to the data identifier and decrypting the data.

It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention and together with the description serve to explain the principles of the invention.

In the drawings:

FIG. 1 is a schematic diagram of an exemplary client/server environment;

FIG. 2 is a schematic diagram showing one embodiment of the wrapper protocol system as an interface between a user and application layer of a network;

FIG. 3 conceptually illustrates a protocol system in the context of the TCP/IP protocol suite;

FIG. 4 shows an embodiment of the present invention as an end-to-end client/server protocol system;

FIG. 5 shows the data segments utilized by one embodiment of the present invention;

FIG. 6 is a flow diagram for securely transmitting and receiving data according to one embodiment of the present invention;

FIG. 7 shows a flow diagram of one embodiment of the present invention for securely transmitting data that conforms to HTTP; and

FIG. 8 shows an HTTP request message.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Certain terminology is used herein for convenience only and is not to be taken as a limitation on the present invention.

Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like elements.

An interface protocol system has application for efficiently and securely transferring data, preferably binary data, between two or more network devices or nodes. By encoding encrypted and unencrypted data segments into a format that conforms to a network protocol, the protocol system acts as an interface protocol between the user, both human and software, and a particular network protocol. The user in this sense includes any computer program operation of a networked device. The term network is broadly construed to include nodes connected by both physical and telecommunication links. A network device or node can be a computer, Personal Digital Assistant (PDA), mobile phone, set-top box, fax machine, printer, or any device capable of sending and/or receiving data generated by other devices on the network.

ENVIRONMENT

Preferably, the system of the present invention operates in a client/server environment. FIG. 1 is a simplified illustration of an exemplary client-server environment, in which features of the present invention may be implemented. A client-server environment, such as the World Wide Web (the Web), is used to communicate information. Web servers and clients, connected to the Internet 120, communicate using a protocol such as Hypertext Transfer Protocol (HTTP). An exemplary Web server 130, that includes a server engine 150, various Web pages

140, and a content database 160, receives HTTP requests from various client systems 100. Using a Web browser 110, such as Netscape Navigator™ or Internet Explorer™, the user requests to access Web pages 140 identified by a URL (Uniform Resource Locator). The Web server 130 responds to the request and/or other queries by providing the requested Web pages 140 to the client system 100. The pages are typically in the form of a text document coded in a standard language such as Hypertext Markup Language (HTML). As shown in FIG.1, one or more clients of different hardware architecture can use the services of one server 130.

PROTOCOL

FIG. 2 shows a conceptual illustration of the protocol system 210 as an interface protocol between the user 200, whether human or software, and the applications layer 220 of a network. The exemplary network shown in FIG. 2, which shows the Transfer Control Protocol/Internetworking Protocol (TCP/IP) suite 270, include applications layer 220, transport layer 230, network layer 240, data link layer 250, and physical layer 260. The layered framework of a network system allows communications across all types of computer systems. However, the protocols of the applications layer 220 determine the data formats for transmitting data. Because many application protocols 220 and proxy servers do not support binary transmissions, the system of the present invention provides an interface protocol 210 for transmitting data, including binary data, that would otherwise not necessarily be supported by one of the available application protocols 220. Moreover, the protocol system of the present invention encrypts and encapsulates

the data in a manner that provides enhanced security in comparison with existing application protocols 220.

FIG. 3 shows one embodiment of the present invention in the context of the layered design of the Internet. Preferably, the protocol system of the present invention 210 acts as an interface between the user 200, whether human or software, and the following application layer protocols 220, which run on top of TCP/IP: HTTP 310, FTP 320, SMTP 330, and SHTTP 340. Of course, one skilled in the art will recognize that application of the present invention is not limited to these protocols 220 and that as new protocols are developed it will be advantageous to support those protocols as well.

Although the protocol system 200 provides for the encryption and encoding of any data type, the preferred embodiment of the present invention is adapted for transmitting binary data. Normally, the input data of an HTML form is transmitted as URL-encoded data using HTTP or SSL. For example, in a survey consisting of 100 yes/no questions, the answers could be sent without indicating the number of the question as HTTP "pair values" (=y&=y&=n . . .). Since three bytes are needed for each answer, 100 answers would require transferring 300 bytes. On the other hand, using binary data to represent the answers to the 100 questions, the data packet size would be significantly reduced. For example, a binary bit could represent each yes/no answer. Therefore, 300 bits or only 37.5 bytes (300/8 bytes) would be required to send the results of the survey. The system of the present invention reduces the amount of data that must be transmitted by encoding binary data into an URL-encoded format supported by the most popular application protocols 220 of the Internet. While the preferred embodiment of the invention is adapted for

transmitting binary data over the Internet, the invention is equally applicable to other wide area networks.

HTTP COMPATIBLE

In one embodiment of the present invention shown in FIG. 4, the protocol system of the present invention functions as an end-to-end client/server protocol. The protocol system, installed at a client **100** and server **130**, connected to the Internet **410**, enable the secure transfer of binary data using HTTP. At the client **100** of FIG. 4, one embodiment of the protocol system **400** serves as a protocol interface for encrypting and preparing binary data in a format that conforms to HTTP. Encoded into a standard HTTP method (or command), the data is transferred to the server **130**, where one embodiment of the protocol system **420** decodes and decrypts the data, thereby restoring it to its original binary state. While the preferred embodiment of the invention discloses transferring binary data from a client to a server, one skilled in the art will appreciate that the present invention is operable for transmitting binary data between any networked devices, including computers, PDA's, printers, fax machines, and mobile telephones.

DATA SEGMENTS

In order to securely and reliably transmit data using existing network protocols, the method and system of the present invention include four data segments **500** or portions shown in FIG. 5. The unencrypted, ASCII packet identifier **510** indicates the type of data encrypted in the third segment **530**. The unencrypted, binary data identifier **520** is used to identify the encryption key used to

encrypt the data contained in the third data segment 530. Finally, the fourth data segment 540 includes data to verify the integrity of transmission.

METHOD

The overall method of the present invention is best understood by reference to the flow diagram shown in FIG. 6. In order to provide secure transfers using existing network protocols, raw binary data is preferably encrypted at 600 with the Data Encryption Standard (DES). One skilled in the art will appreciate that any appropriate encryption scheme utilizing an encryption key can be utilized. At 610 a data identifier 520, preferable unencrypted and in a binary format, is associated with the encryption key used in the encryption process 600. Then at step 620, which is interchangeable with step 610, an unencrypted and character-based packet identifier 510 identify the data segments 500 as having been encoded according to the protocol of the present invention. The packet identifier 510 also indicates the type of data (e.g. binary) encrypted at 600. Alternatively, the packet identifier 510 may also include data to indicate the type of computer system that was used to prepare and transmit the data segments 500. Then, when the data segments 500 are later received and decoded, the protocol system can determine whether the data should be converted to a format compatible with the recipient's computer system (big-endian to little-endian). Therefore, the system of the present system is compatible with different computer systems including, but not limited to, Macintosh™, IBM-PC compatibles, and SUN Solaris™ servers.

A fourth data segment utilized by the protocol system is created at 630 to include data integrity checks 540 or codes for verifying the integrity of the data after

transmission. Preferably, the system of the present embodiment includes a cyclic redundancy check (CRC) and an internal data integrity code. After the binary data has been encrypted and the other data segments created, the data segments 500 at step 640 are encoded to conform to a particular network protocol. This usually entails converting the encrypted binary data and the binary data identifier into an ASCII or URL-encoded format. The non-binary data segments are also converted into a format supported by a particular application protocol 220.

At 650 the data segments 500 are transmitted according to the standards of the application protocol 220. Also at 650, the encryption key is sent, preferably off-line, to the recipient of the data transmission. The recipient network device receives the data transmission and decodes the data segments 500 at 660. Using the data identifier 520, the recipient retrieves the appropriate encryption key 670 and decrypts the binary data 680.

CLIENT

With reference to the FIG. 4, one embodiment of the protocol system 400 that encrypts and configures data that conforms to HTTP standards is shown in more detail in FIG. 7. The present embodiment includes the encryption 600 of binary data 700, the constitution and encoding 640 of four data segments 500 into a standard HTTP format 720. As will be appreciated by one skilled in the art, the data segments 500 of the present invention alternatively can be encoded 640 for other network protocols 220 including, but not limited to, the FTP, SHTTP, and SMTP protocols. Both binary data segments, the data identifier 520 and the encrypted binary data 530, are converted to an URL-encoded format. Finally, the four data

segments are configured or arranged such that the data segments conform to a standard HTTP method.

FIG. 7 illustrates the data segments **500** encoded at **640** into a "pair value" format **720** compatible with standard HTTP GET/POST methods. The HTTP is mainly used to access and retrieve URL-named resource on the Web. An HTTP client/server session consists of a single request/response interchange. The client initializes a connection to a remote server by sending a request message. The server processes the request, returns a response message to the client, and closes the connection. The request message **800**, shown in FIG. 8, consists of a request line **810**, one or more optional headers **820**, and an optional entity body **840**. The entity body **840** is preceded by a blank line **830**. Methods (or commands) from the client to the server are included in the request line **810** of the request message **800**. Common HTTP methods are GET, which retrieves identified information, and POST, which requests the server to accept the entity body **840** enclosed in the request **800**. For example, using the POST method, a client can send HTML form's data to the specified URL.

Since raw binary data is not compatible with HTTP GET transfer, the present embodiment of the invention encodes **640** and configures the data segments **500** of FIG. 7 into a "pair value" format **720**. Typically, in the client/server environment known as the Web, input data from a HTML form is collected by the user's browser and transmitted to a Web server. The input data, contained in one or more data entry fields of an HTML page, is sent to the Web server by invoking an HTTP method. When activated, the user's Web browser retrieves the data within the HTML form and assembles the data into one long string of "pair values" (i.e. "name=value"

separated by an ampersand (&)). Each "pair value" is URL-encoded by changing spaces into pluses and by encoding some characters into hexadecimal. In the present embodiment, the data segments **500** would take the following format:

PacketIdentifier=DataIdentifier&EncryptedData=IntegrityData

The Web browser invokes an HTTP GET or POST method and transmits the data to the server. When using the GET method, the "pair values" are appended to the URL. In contrast, if the POST method is used, the "pair values" are sent in the body **840** of the request message **800**.

SERVER

The server receives and parses the HTTP request message **800**, which preferably includes the name of a Common Gateway Interface (CGI) program. In the example of a POST method, the server recognizes the POST method and initiates communication with the CGI program. Using techniques well known in the art, the message body is transmitted to the CGI program that parses the message containing the "pair values." As disclosed above, the present embodiment of the protocol system then decodes the data segments **500** into their original data formats, retrieves the encryption key associated with the data identifier, and decrypts the binary data.

Although the present embodiment of the present invention is discussed in the context of a Web browser plug-in, in alternative embodiments of the invention the system is implemented as a stand-alone application, or as an enhancement to an existing software application.

In an alternative embodiment the protocol system can be used to facilitate the transfer of data along a network path. For instance, instead of providing an interface protocol between two end nodes of a network, the wrapper protocol system alternatively can be implemented to receive data according to the protocol system of the present invention and forward it to another network device. At the intermediate network device, the data also can be manipulated before being forwarded along to an end-user.

It will be apparent to those skilled in the art that various modifications and variations can be made in the method and system for transmitting data of the present invention without departing from the spirit or scope of the invention. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What Is Claimed Is:

1. A method for transmitting data with enhanced security that conforms to a network protocol, the method comprising:

providing data segments including a first segment having encrypted data, an unencrypted packet identifier identifying the encrypted data, an unencrypted data identifier associated with an encryption key used to encrypt the encrypted data in the first data segment, and a fourth data segment having data to verify integrity of transmission;

encoding the data segments to conform to a network protocol;

transmitting the data segments and encryption key;

receiving and decoding the data segments; and

decrypting the encrypted data using the encryption key that corresponds to the data identifier.

2. The method of claim 1, wherein the fourth data segment includes a cyclic redundancy check (CRC).

3. The method of claim 1, wherein fourth data segment includes at least one internal integrity check.

4. The method of claim 1, wherein the unencrypted data identifier is in an encoded binary format.

5. The method of claim 1, wherein the unencrypted packet identifier is in an ASCII format.

6. The method of claim 1, wherein the unencrypted packet identifier is URL-encoded.

7. The method of claim 1, wherein the encrypted data includes encoded binary data.

8. The method of claim 1, wherein the unencrypted data identifier is in an encoded binary format.

9. The method of claim 1, wherein the unencrypted data identifier can be used as a file header.

10. The method of claim 1, wherein the step of providing a data segment having encrypted data further comprises the step of encrypting the data.

11. The method of claim 10, wherein encrypting the data includes encrypting the data with binary encryption.

12. The method of claim 11, wherein encrypting the data with binary encryption includes encrypting the data with DES encryption

13. The method of claim 1, wherein the unencrypted packet identifier includes information about a computer system that generated the unencrypted packet identifier.

14. The method of claim 13, further comprising the step of converting the transmitted data based on a computer system information from a big-endian to a little-endian format after the data has been decoded.

15. The method of claim 1, wherein encoding the data segments to conform to a network protocol includes encoding binary data to a URL-encoded format.

16. The method of claim 1, wherein encoding the data segments to conform to a network protocol includes arranging the data in a format compatible with the network protocol.

17. The method of claim 16, wherein arranging the data in a format compatible with the network protocol includes arranging the data to conform to at least one or more of HTTP, FTP, SMTP, and SHTTP.

18. The method of claim 1, wherein encoding the data segments to conform to a network protocol includes encoding the data segments to conform to an HTTP GET or POST method.

19. The method of claim 18, wherein encoding the data segments to conform to an HTTP GET or POST method includes encoding the data segments into a format "PacketIdentifier=DataIdentifier&EncryptedData=IntegrityData".

20. The method of claim 1, wherein the step of transmitting the encryption key includes sending the encryption key offline.

21. The method of claim 1, wherein the network protocol includes one or more of a HTTP, FTP, SMTP, and SHTTP.

22. The method of claim 1, wherein decoding the data segments includes parsing the data segments.

23. The method of claim 1, wherein decoding the data segments includes reading the packet identifier without having to decode the other data segments.

24. The method of claim 1, wherein decoding the data segments includes reading the data identifier without having to decode the other data segments.

25. The method of claim 1, wherein decrypting the encrypted data includes reading the data identifier and retrieving the encryption key associated with the data identifier.

26. A system for transmitting data with enhanced security that conforms to a network protocol, the system comprising:

means for encrypting data with an encryption key and associating a data identifier with the encryption key;

means for associating a packet identifier with the encrypted data;

means for encoding the packet identifier, data identifier, and data into a format compatible with a network protocol;

means for receiving and decoding the packet identifier, data identifier, and data; and

means for retrieving the encryption key that corresponds to the data identifier and decrypting the data.

27. The system of claim 26, wherein the means for associating a data identifier with the encryption key includes creating an encoded binary data identifier.

28. The system of claim 26, wherein the means for associating a data identifier with the encryption key includes creating an unencrypted data identifier.

29. The system of claim 26, wherein the means for associating a packet identifier with the encrypted data includes creating an unencrypted packet identifier.

30. The system of claim 26, wherein the means for associating a packet identifier with the encrypted data includes creating the packet identifier in ASCII format.

31. The system of claim 26, wherein means for encrypting data with an encryption key includes encrypting the data with binary encryption.

32. The system of claim 31, wherein means for encrypting the data with binary encryption includes encrypting the data with DES encryption.

33. The system of claim 26, wherein the means for encoding the packet identifier, data identifier, and data into a format compatible with a network protocol includes encoding the packet identifier, data identifier, and data into a URL-encoded format.

34. The system of claim 26, wherein the means for encoding includes encoding binary data into URL-encoded data.

35. The system of claim 26, wherein the means for decoding the data identifier and data includes converting the data identifier and data into an encoded binary format.

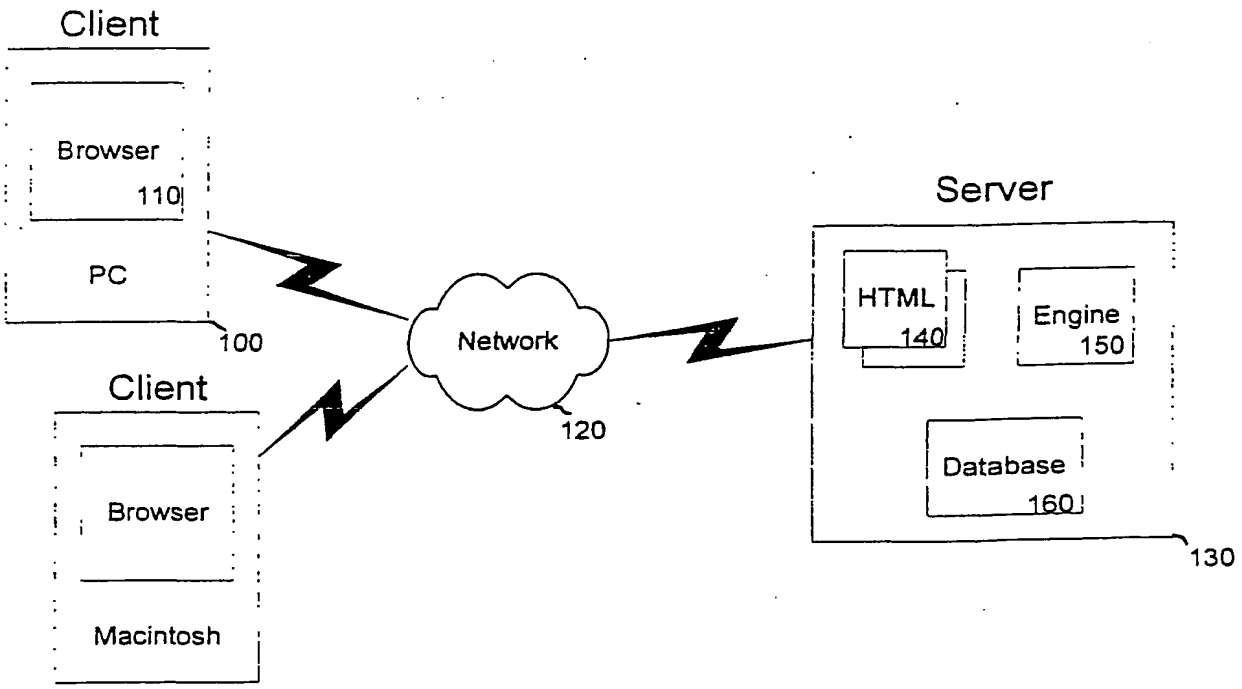
Client
Browser
110
PC
100
Client
Browser
Macintosh
Network
120
Server
HTML
140
Engine
150
Database
160
130

FIG. 1

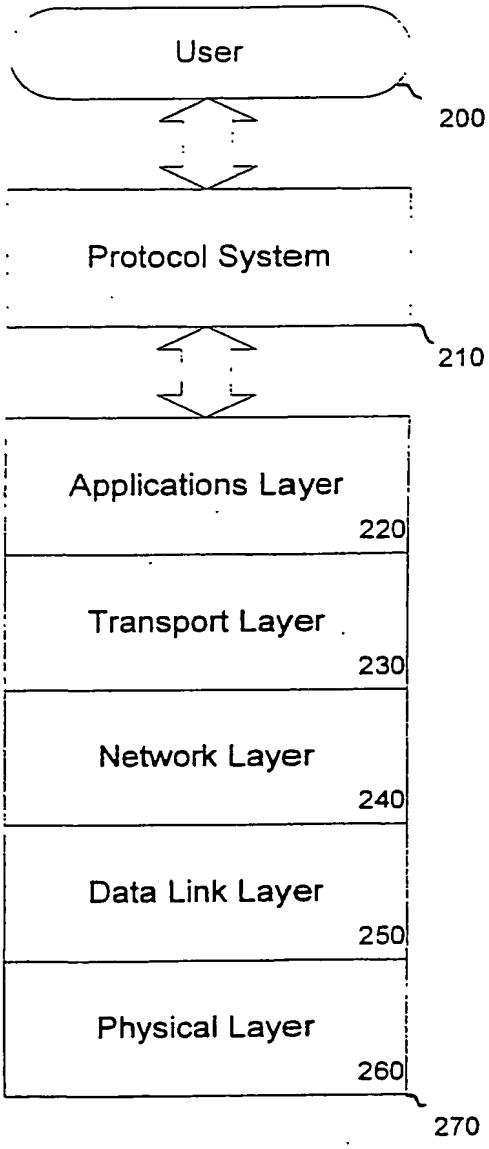
User
200
Protocol System
210
Applications Layer
220
Transport Layer
230
Network Layer
240
Data Link Layer
250
Physical Layer
260
270

FIG. 2

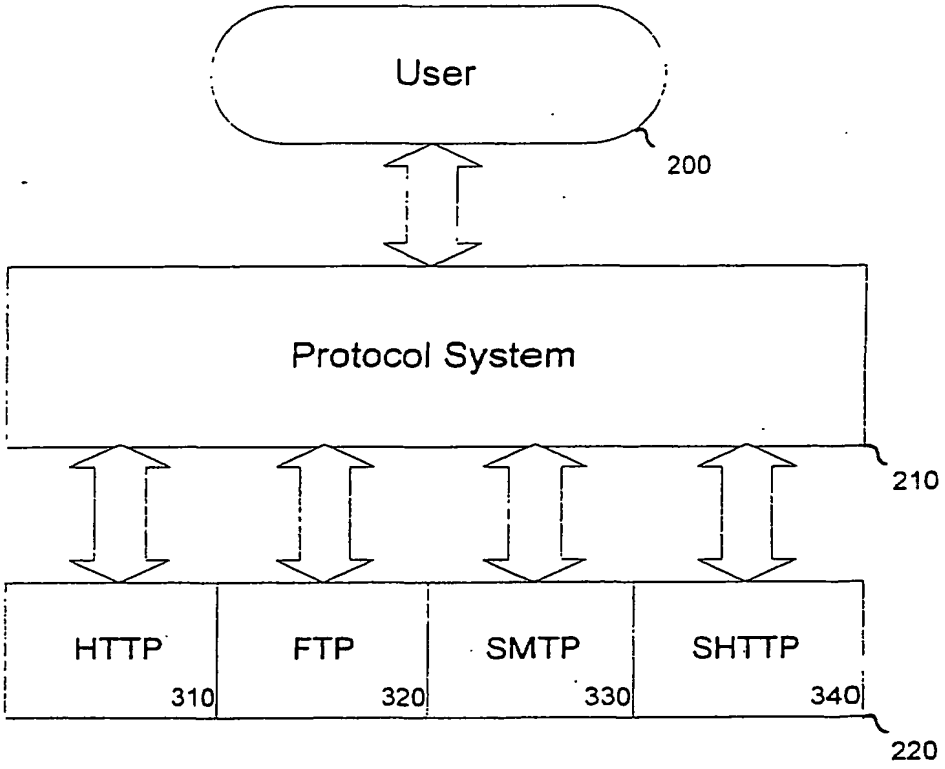
User
200
Protocol System
210
HTTP
310
FTP
320
SMTP
330
SHTTP
340
220

FIG. 3

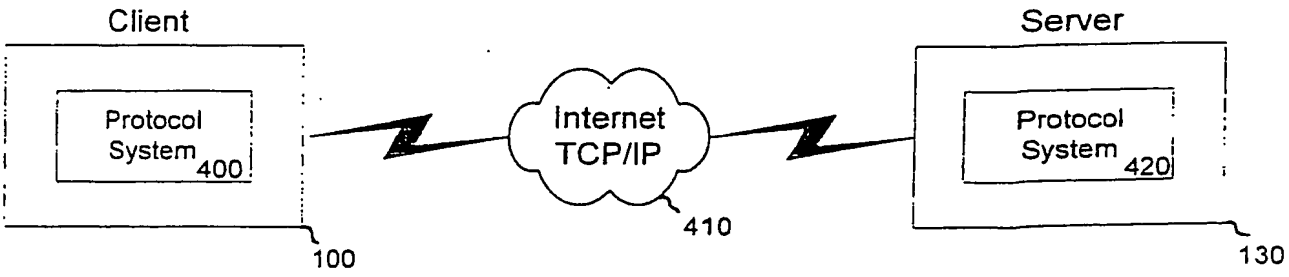
Client
Protocol System 400
100
Internet TCP/IP
410
Server
Protocol System 420
130

FIG. 4

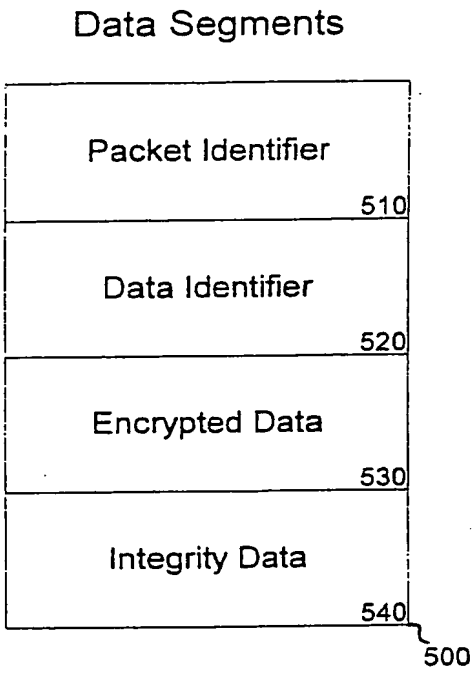
Data Segments
Packet Identifier
510
Data Identifier
520
Encrypted Data
530
Integrity Data
540
500

FIG. 5

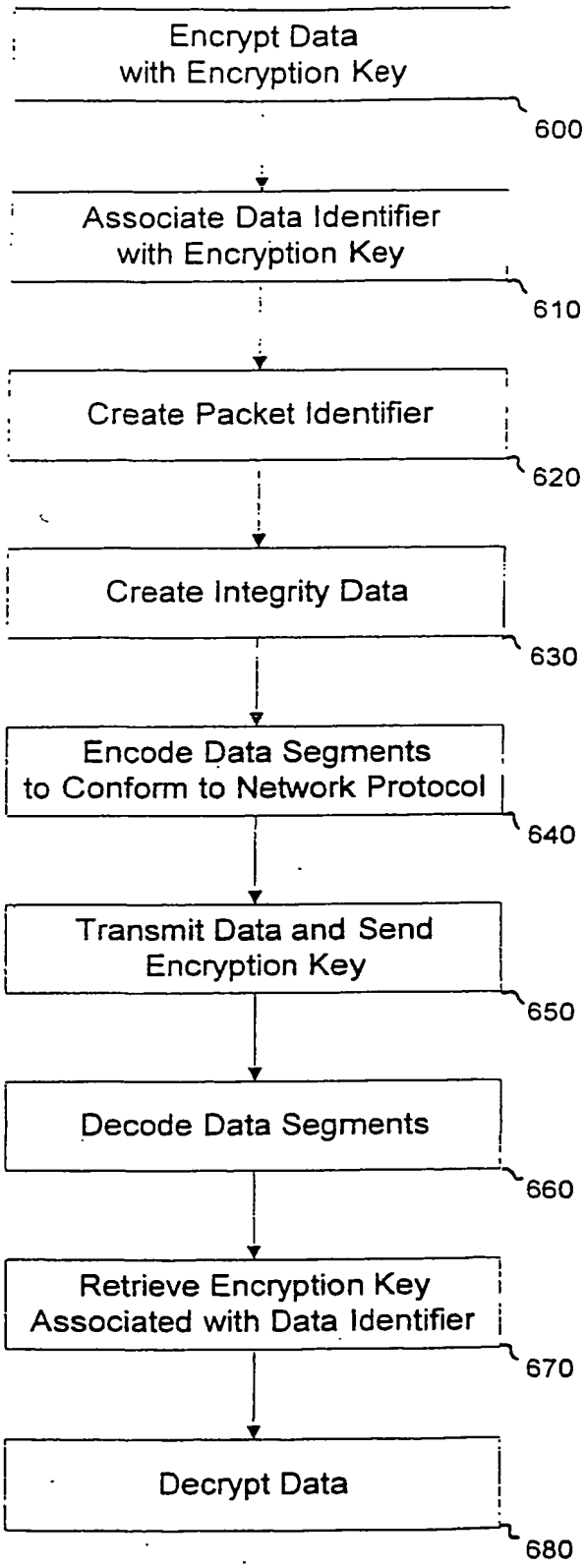
Encrypt Data with Encryption Key
600
Associate Data Identifier with Encryption Key
610
Create Packet Identifier
620
Create Integrity Data
630
Encode Data Segments to Conform to Network Protocol
640
Transmit Data and Send Encryption Key
650
Decode Data Segments
660
Retrieve Encryption Key Associated with Data Identifier
670
Decrypt Data
680

FIG. 6

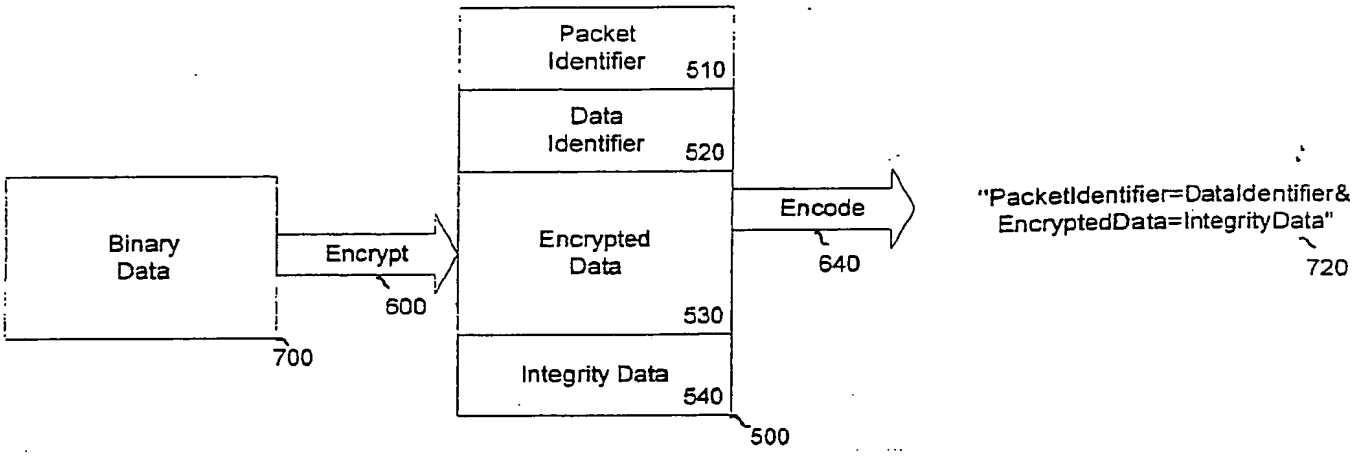
Packet Identifier
510
Data Identifier
520
Encrypted Data
530
Integrity Data
540
500
Binary Data
700
Encrypt
600
Encode
640
"PacketIdentifier=DataIdentifier&
EncryptedData=IntegrityData"
720

FIG. 7

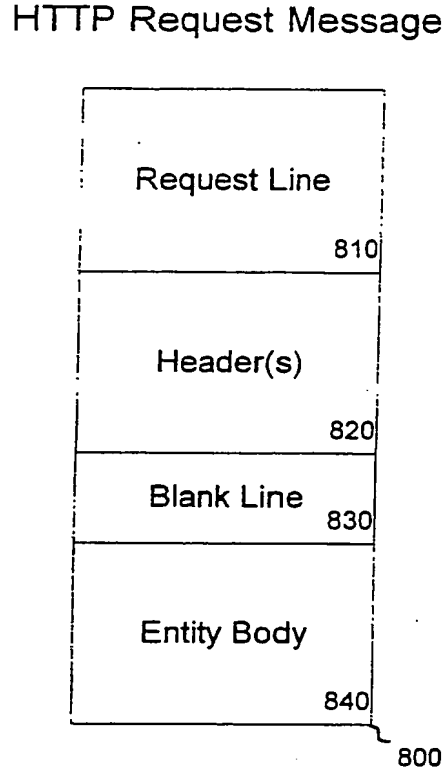
HTTP Request Message
Request Line
810
Header(s)
820
Blank Line
830
Entity Body
840
800

FIG. 8